

not available to the public (or available at prohibitive cost). Bank notes are a common example. Producing an unforgeable document usually entails using special paper and/or special printing. (Special papers include paper with colored or forensic fibers, paper with transparent windows, paper with holograms, and paper with watermarks. Special printing means high-resolution printing of text or special patterns that do not accurately reproduce on most photocopiers.)

**[0078]** Cryptographic checksums (usually over 100 binary digits long) are known as message digests, message authentication codes, integrity check-values, modification detection codes, or message integrity codes. Currently, cryptographic checksums are either 128 or 160 bits (binary digits) long. Assuming octal encoding, this can be represented by 32 or 40 decimal digits. This size is considered unbreakable for the near future (say the next 5-10 years). As computers become more powerful, the size will be increased (such as doubled). A cryptographic checksum is a mathematical value (called a checksum) that is assigned to a file and used to "test" the file at a later date to verify that the data contained in the file has not been maliciously (or accidentally) changed. A cryptographic checksum is created by performing a complicated series of mathematical operations (defined by a cryptographic algorithm) that takes as inputs the data in the file and a cryptographic key (a randomly-chosen large number, e.g., 50 to 100 binary digits) and outputs a fixed string of digits, which is then used as a checksum. The cryptographic algorithm itself is not usually secret. But the cryptographic key is secret. Without knowing the key, it is highly unlikely (i.e., computationally unfeasible) that one can change the data in the file and obtain the appropriate checksum.

**[0079]** A printed certificate may be desired to be unmodifiable but not necessarily unforgeable. For example, any transaction involving the certificate will be handled through a designated financial institution that keeps track of which certificates are outstanding and who their owners are. Whereas a printed certificate that can be traded like money (i.e., anonymously) has to meet the stronger condition of being unforgeable.

**[0080]** Cryptographic checksums are in a digital form to be transmitted electronically in data transmission and data storage. A cryptographic checksum usually stored on disk or flash (both non-volatile storage) or RAM (volatile).

**[0081]** The current credit cards, id cards, and similar cards with magnetic stripes only use digital codes, but not cryptographic checksums. Smart cards have a processor and memory (volatile and non-volatile) for storing cryptographic quantities and executing cryptographic algorithms. But these quantities are not printed on the card or a hardcopy document.

**[0082]** Other certificates, such as driver licenses, passports, etc. only contain printed codes, such as digits, 2D or 3D bar codes, but not cryptographic checksums. The latest passports may incorporate smart card technology, but not any cryptographic checksum printed thereon.

**[0083]** The invention scans the cryptographic checksum printed on a hardcopy certificate, checks its validity with the ASD host **101** (or financial institutions underwriting or transacting securities), and accepts the certificate only if the cryptographic checksum matches.

**[0084]** Alternatively, the purchaser may designate a depository, such as a security breakage company or the like which the purchaser has an account with. In one embodiment of the invention, the issuing machine **105** also functions as an automatic teller machine (ATM) or other kiosks, such as paying routine bills, fees, and taxes (utilities, phone bills, social security, legal fees, taxes, etc.), loading monetary value into pre-paid cards (cell phones, tolls), conducting ticketing transactions (train, concert, etc.).

**[0085]** The issuing machine **105** may have custom circuit boards or use a computer with special software running on operating systems such as Windows, Linux, etc. The computer (a CPU, a RAM, a ROM, a disk, etc.) runs the software (operating system, applications) which controls the operation of the ASD.

**[0086]** The ASD **105** interacts with customers via input-output devices including keypad, display, card reader, and document printer-scanner. The ASD host **101** is part of a network of securities dealing financial institutions, and all interactions between the ASD **105** and the securities dealing financial institutions are handled via the ASD **105** host.

**[0087]** The ASD **105** interacts with the ASD host **101** via a communication link such as a dial-up line, leased-line, or local area network connected to the Internet. The ASD **105** also has the cryptoprocessor which executes the cryptography software for achieving secure communication between ASD **105** and ASD host **101** (and any other cryptographic operations needed). The ASD **105** has a backup battery to ensure normal operation and proper closing in the event of power failure. In-store issuing machine **105** may have its cryptoprocessor connected directly to the internet or other network, or via a modem over a dedicated telephone line then to the internet so as to connect to the server. The secure crypto processor is generally within a computer in a secure enclosure. The security of the issuing machine **105** relies on the integrity of the secure cryptoprocessor.

**[0088]** If appropriate, the issuing machine **105** then, by means of an issuing function, (1) prompts a pop-up screen for users to click-through to indicate whether they are located within a jurisdiction where the offering has been registered or is exempt from registration, or the site may be password-protected for investors who have otherwise been screened and given passwords, (2) prompts a pop-up screen for users to click-through to consent to electronic delivery/display a statutory prospectus, and to acknowledge that they have electronically received/reviewed the statutory prospectus, and then (3) issues the securities **107** based on the corresponding securities purchase offer information. The issuing machine **105** also prompts a statement that paper copies of the prospectus and other required SEC documents are available upon request from an identified contact. The issuing machine **105** also has an issue result transmitting function which is used to transmit confirmation of the securities issue to the server **101** as the security issue result information or confirmation.

**[0089]** Optionally, the server **101** and the issuing machine **105** supports real-time pricing for newly-issued securities on-line to the public based upon the offers to purchase and offers to sell available real-time, rather than traded on a regular, periodic basis, such as weekly, semi-weekly, or daily like in the current bond market.

**[0090]** Outdoor issuing machines **105** may be free-standing, like a kiosk, or built into the side of a building of